



Uluslararası Sosyal Araştırmalar Dergisi

The Journal of International Social Research

Cilt: 8 Sayı: 41 Volume: 8 Issue: 41

Aralık 2015

December 2015

www.sosyalarastirmalar.com ISSN: 1307-9581

**SİBER UZAMA YÖNELİK GÜVENLİKÇİ SÖYLEMİN İNŞASI: SONY PICTURES'A YÖNELİK
SİBER SALDIRI HABERLERİNİN ANALİZİ
CONSTRUCTION OF CYBER SECURITY DISCOURSE: ANALYSIS OF SONY PICTURES HACK
NEWS**

Sevda ÜNAL*

Öz

Bu çalışmada Sony Pictures'a yönelik siber saldırının ABD medyasında sunumu incelenmiştir. Bu kapsamda liberal ve muhafazakâr eğilime sahip olan iki ABD gazetesinin Sony Pictures'a yönelik siber saldırıya ilişkin haberleri sunumunda egemen söylemlerin kuruluşu ve işleyişi siber güvenlik söylemi bağlamında ele alınmıştır. Çalışmada medya kuruluşlarının uzama yönelik siber terör tehdidinin sadece yayılmasına değil aynı zamanda bu tehdidin söylemsel inşasına da önemli ölçüde katkı sağladığı argümanından hareket edilmektedir. Terör tehdidinin söylemsel inşası beraberinde terörle mücadele söylemini de getirmektedir. Bu söylemlerin inşası Fairclough'un eleştirel söylem analizi yöntemiyle çözümlenmeye çalışılmıştır.

Anahtar Kelimeler: Siber Güvenlik, Siber Terör, Haber Medyası, Sony Pictures, Eleştirel Söylem Analizi.

Abstract

In this study representation of cyber attacks against Sony Pictures at US media was studied. Within this framework, with liberal and conservative bias two US newspapers was chosen. The construction and functioning of dominant discourse during the of cyber attack against Sony Pictures was analysed in the context of cyber security. In this study the main argument is media outlets not only contribute to the dissemination of cyber terrorism threat but also contribute discursive construction of this threat. The discursive construction of terrosim threat bring with counterterrorism discourse. The construction of terrorism discourse was analysed by critical discourse analysis method. Norman Fairclough's critical discourse analysis method was chosen as a research method of this study.

Keywords: Cyber Security, Cyber Terrorism, News Media, Sony Pictures, Critical Discourse Analysis.

Giriş

Siber uzam ve dolayısıyla İnternet modern yaşamın merkezindedir. İnternet iş dünyası, ekonomi, siyaset ve toplumlar için önemli bir araç haline gelmiştir. Pek çok ülkenin enformasyon ve iletişim teknolojilerinin kullanımının artışına paralel olarak siber uzama bağımlılıkları da artmıştır.

Soğuk Savaşın sona ermesiyle birlikte bilişim sistemlerinin satılmasına ve teknoloji aktarımına yönelik sınırlamaların kalkması, İnternetin sivilleşmesi ve aynı zamanda ticari ve toplumsal kullanıma açılması sürecini hızlandırmıştır. Böylece dijital verilen aktarıldığı, verilerin işlenebildiği siber uzam olarak adlandırılan sanal bir dünyanın yolu açılmıştır. Ancak siber uzamın ekonomik, politik, toplumsal ve askeri alanlarda kullanılmasının sağladığı olanaklar beraberinde yeni güvenlik sorunlarını da getirmiştir (Bıçakçı, 2013: 2-3). Siber uzamın önemli bir parçası olan İnternetin gelişen teknolojiyle birlikte kritik altyapılar olarak sistemlere entegre edilmesi, İnternetin ticari kullanıma açılmasıyla sürdürülebilir ekonomik refahın önemli bir parçası haline gelmesi, terörizm ve kritik altyapıların korunmasıyla ilişkilendirilmesi siber uzamın güvenliği konusunu siyasi gündeme yerleştirmiştir.

İnternet ve ağ teknolojilerinin toplumsal kullanıma açıldığı 1990'ların ortalarından itibaren ABD'den başlayarak siber uzama yönelik güvenlik politikaları ulusal güvenliğin bir parçası olarak ele alınmaya başlamıştır. Siber uzama yönelik güvenlik merkezli söylemin temellerinin atılması, konunun kritik altyapıların korunması ve dolayısıyla siber uzamla bağlantılandırılmasında 1995 yılında ABD'nin Oklahama şehrinde gerçekleştirilen bombalı saldırı ve 11 Eylül 2001'de Dünya Ticaret Merkezi'ne gerçekleştirilen terör saldırıları önemli dönüm noktaları olmuştur. Kısaca Soğuk Savaş sonrasında, döneme ait tehdit senaryolarının geçerliliğini yitirmesi, nereden geleceği ve kim ya da kimler tarafından gerçekleştirileceği belli olmayan asimetrik tehdidin hakimiyet kazanması askeri açıdan da yeni risk ve tehdit tanımlamalarının yapılmasına neden olmuştur. Bu kapsamda siber uzama yönelik güvenlik eksenli söylemin inşasında siber uzam kaynaklı ve siber uzama yönelik terör saldırılarının neden olabileceği yıkım ve felaketler politikacılar ve medya aracılığıyla sürekli pompalanarak bir korku ortamı oluşturulmuş; yaratılan bu korku atmosferiyle güvenlik adına özgürlüklerden feragat edildiği yeni bir dönemin önü açılmıştır. Özellikle ABD'de bu korku ortamı ABD toplumunun yaşadığı felaketlere atıfta bulunan "Dijital Pearl Harbour", "Dijital 11 Eylül" gibi

* Doktora Öğrencisi, Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Gazetecilik Ana Bilim Dalı.

metaforlar aracılığıyla pekiştirilmiştir. Böylece geleneksel güvenlik önlemlerinin siber uzama uygulanmasının da önü açılmıştır.

Siber uzama yönelik güvenikleştirme söyleminin inşasında, bu kapsamda yapılacak uygulamalara ulusal ve uluslararası kamuoyu nezdinde meşruiyet kazandırmada politikacıların açıklamaları, medya organları, resmi politika belgeleri ve raporlar önemli rol oynamaktadır. Öyle ki bir politika alanındaki hakim söylem, bu politika alanıyla ilgili bilginin nasıl anlaşılması ve yorumlanması gerektiği konusundaki algımızı şekillendirmektedir. Böylece hakim söylemler politika alanının çalışmasını ve altta yatan ideolojiyi yönetmeye, şekillendirmeye ve güçlendirmeye hizmet eden “gerçeklikler” üretmektedir. Söylemsel kurgular geniş toplumsal yapılara nüfuz etmekte, toplumun belleğinde gerçeklikler somutlaşmakta ve toplumsal konuların nasıl algılanması gerektiği konusundaki statüko tesis edilmektedir. Medyada siber güvenlik söyleminin çerçevelenmesi ve şekillendirilmesinde önemli bir araç olarak öne çıkmaktadır. Medya metinleri aracılığıyla kendini söylemde açığa çıkaran güvenikleştirme, sorunların varoluşsal tehditler gibi tasvir edilmesi ve daha sonra ilgili kitlenin ikna edilmesi yoluyla gerçekleşmektedir.

Siber uzama yönelik güvenikleştirme söyleminin meşrulaştırılmasında uzama yönelik saldırıların medya tarafından ele alınma tarzı da önemli bir işleve sahiptir. Özellikle 11 Eylül 2001 terör saldırısı, 2007 yılında Estonya devleti İnternet ağlarına, 2008 yılında Rus-Gürcü savaşı sırasında Gürcistan’ın resmi İnternet sitelerine yapılan saldırılar ve 2010 yılında İran’ın Nataz’daki nükleer tesislerine yapılan Stuxnet saldırısı siber uzama yönelik saldırıların ulusal güvenlikle ilişkilendirilmesi ve bu saldırıların terör saldırısı kapsamında ele alınmasının önünü açmıştır. Böylece uzama yönelik güvenikleştirme faaliyetlerinin meşrulaştırılmasında siber savaş, siber terör, siber suç gibi kavramlar siyasi ve askeri literatürde yerini almıştır.

Siber uzama yönelik ve siber uzam kaynaklı risk ve tehditlerin toplumun fiziksel, kültürel ya da sosyal sağlığı açısından yakın bir varoluşsal tehdit oluşturduğu algısı yaratılmış, ancak bu tehditler keşfedilmesi gereken belirli gerçeklikler olarak ele alınmamış, güvenikleştirme olarak adlandırılan sosyo-politik bir süreçte söylem aracılığıyla inşa edilmiştir. Bu inşa sürecinde öncelikle uzama yönelik herhangi bir saldırı politikacıların söylemleri ve medya aracılığıyla terör saldırısı kapsamında değerlendirilmekte ve kritik altyapıların güvenliğiyle ilişkilendirilmektedir.

Çalışmada medya kuruluşlarının uzama yönelik siber terör tehdidinin sadece yayılmasına değil aynı zamanda bu tehdidin söylemsel inşasına da önemli ölçüde katkı sağladığı argümanından hareket edilmektedir. Terör tehdidinin söylemsel inşası beraberinde terörle mücadele söylemini de getirmektedir. Terörle mücadele söylemi çerçevesinde uzama yönelik düzenlemelere meşruiyet sağlanmaktadır. Bu kapsamda çalışmada Sony Pictures’a yönelik siber saldırıya ilişkin haberler aracılığıyla bu inşa sürecinin ortaya çıkarılması amaçlanmaktadır.

1. Olayın Özeti

Sony Pictures’ın bilgisayar ağlarına yönelik saldırı kendilerini “Barışın Bekçileri” (Guardians of Peace) olarak adlandıran bir hacker grubu tarafından 24 Kasım 2014’te gerçekleştirilmiştir. Saldırının nedeninin Sony Pictures’ın yapımcısı olduğu 25 Aralık 2014’te vizyona girecek, Kuzey Kore liderine yapılan bir suikastın konu edildiği “Interview” adlı filmin yayını engellemek olduğu iddia edilmiştir. Bu iddia daha önce Kuzey Kore tarafından yapılan “filmin yayınlanması savaş ilanı olur” şeklindeki açıklamalarına dayandırılmıştır.¹

2. Araştırmanın Yöntemi

Gazete söylemi, dilin taraflı kullanımını ortaya çıkarmak ve dilin nasıl manipüle edildiği hakkında okuyucunun farkındalığını artırmak amacıyla aslında çok uzun zamandır pek çok eleştirel söylem analistçisinin odak noktası olmuştur. Eleştirel söylem analizi perspektifine göre gazeteler sosyal ve siyasi perspektiflerine dayalı olarak farklı olayları ve olguları tasvir ederler. Yani medya söylemi gizli ideolojiler ve manipüle edilmiş söylem yapıları içine gömülmüştür. Benzer şekilde Entman (2007) ve Fairclough (2003)’a göre medyanın izleyicilerde hangi ideolojinin temsil edileceğini ve güçlendirileceğini belirleme rolü vardır. Fairclough’a göre başka birinin sesi metnin içine dahil edildiğinde metnin diğer bölümleri açısından nasıl bağlamsallaştırılacağı, nasıl çerçeveleneceği konusunda her zaman seçenekler vardır (2003: 53). Medya ve politikacıların izleyicilerin ve kamuoyunun ilgisini çekme taktiklerini tartışırken Hall ve Fairclough, medyanın resmi bakış açılarını kamuoyuna iletme ve çeşitli kamuların anlayışına göre onları doğallaştırma konusunda medya eğilimini göstermek amacıyla “doğallaştırma” kavramını kullanmaktadır (Fairclough ve Hall’dan akt. Marko, 2013). Buradaki varsayım, insanların kendi beklentileri ve ortak duyularıyla uyum içindeki bilgileri ve mesajları tercih ettikleridir. Hall’a göre, en doğallaşmış şeyler bazı toplumların tüm üyeleri tarafından verilen ortakduyuyla ilişkilidir (Hall’dan akt. Marko, 2013: 205). Medyanın rolü önemlidir

¹ Saldırıya ilişkin ayrıntılar için bkz. Gök. D., (2014) “Başlangıcından Bugüne Tüm Detaylarıyla ‘Sony Pictures’ Hack Skandalı, <http://onedio.com/haber/baslangicindan-bugune-tum-detaylariyla-sony-pictures-hack-skandali-422621>.

çünkü medya haber olaylarını pasif bir şekilde tanımlamaz ya da kaydetmez ama aktif bir şekilde birçok söylem türünden yola çıkarak yeniden inşa eder. Medyanın toplumsal işlevi güçlünün sesini ortaktuyunun sesi olarak kabul ettirerek mevcut asimetrik güç ilişkilerini üretmek ve meşrulaştırmaktır (Fairclough, 1995: 63). Eleştirel söylem analizi sadece “ne” ve “nasıl”la ilgilenmez, “niçin” ve “kiminle” de ilgilenir. Temel ilgi alanı metnin içine gömülü gizli gündemi, ideolojileri ve düşünceleri belirlemektir. Fairclough’a göre (1992: 113) gazetecilik güç ve ideoloji tarafından şekillenen bir alandır ve sırasıyla insanların sosyal yaşamlarını ve bilgilerini etkiler. Medya metinleriyle ilgili olarak bu metinler her zaman ideolojiler ve yaratıcılarının görüşlerinden etkilenir. Sadece yazarların değil yayıncı, editör, olası yorumcular, yayın şirketinin sahibi ve ortaklarından da etkilenir. Medya metinleri okuyucularına bilgi verirken, aynı zamanda okuyucularının dünya görüşünü ve düşüncelerini inşa etme ve değiştirmede de önemli rol oynarlar. (Markkula, 2014: 11).

Eleştirel söylem analizinin, siber uzama yönelik terör tehdidi söyleminin inşasında haber medyasının rolünü sorgulayan bu çalışmanın kaygılarına yanıt vereceği değerlendirilmektedir. Çalışma eleştirel söylem analistçilerinden Norman Fairclough’un “betimleme, yorumlama ve açıklama” şeklindeki üç boyutlu çerçevesinde yapılandırılmıştır. Betimleme metnin dilsel olarak analiz edilmesi demek olup, metindeki kelimeler, gramer yapısı, anlam, ses, cümle seviyesinde uyum analizi yapmayı gerektirir. Yorumlama boyutu hem toplum ve kültür hem de söylem, dil ve metin arasındaki ayrım üzerinde durur. Bu boyut metinsel ile toplumsal ve kültürel; metin ve sosyokültürel pratik arasında arabuluculuk yapar, bu anlamda sosyokültürel ve metin pratiği arasındaki bağ söylem pratiği yolu ile doğrudan kurulan bir bağıdır. Açıklama boyutu ise iletişimsel bir olayın sosyo-kültürel bağlamının ekonomik, politik (güç ve ideoloji konularıyla ilgilidir) ve kültürel (kimlik ve değer sorularıyla ilgilidir) olmak üzere üç boyutu ile ilgilidir (Fairclough, 1995: 62). Bu çalışmada “betimleme-yorumlama-tanımlama” şeklindeki sıra takip edilmemiş, Fairclough’un Thatcherçi söylem analizi (1996) rehber alınarak tarihsel toplumsal bağlamın ele alındığı açıklama boyutuyla analize başlanmıştır.

3. Araştırma Evreni ve Örnekleme

Sony Pictures’a yönelik siber saldırının gazetelerde sunumunu ele alan bu çalışmanın evrenini Amerikan yazılı basını oluşturmaktadır. Örnekleme olarak Washington Post ve Washington Times gazeteleri seçilmiştir. Liberal bir eğilime sahip² olan Washington Post gazetesi, demokrat Stilson Hutchins tarafından Washington D.C.de 1877 yılında kurulmuştur. Gazetenin sahibi The Washington Post Company’dır.³ Ancak gazete Amazon.com kurucusu ve CEO’su Jeffrey P. Bezos resmen tarafından 1 Ekim 2013 tarihinde satın alınmıştır. 1982 yılında Washington D.C.de kurulan ve günlük bir periyoda sahip olan gazete muhafazakar bir eğilime sahip olup Washington Post’un liberal eğilimini dengelemeyi amaçlamaktadır.⁴ Gazete, Unification Kilisesinin rahibi Sun Myung Moon tarafından ve şirketi News World Communications aracılığıyla kurulmuştur.⁵ Washington Times’ın editoryal eğilimi belirgin şekilde muhafazakâr ve Cumhuriyetçi Parti yanlısıdır.⁶ Söz konusu gazetelerin İnternet sitelerinde - www.washingtonpost.com ve www.washingtontimes.com - yer alan Sony Pictures’a yönelik saldırı haberleri araştırma birimini oluşturmaktadır.

Araştırmada farklı siyasi eğilime sahip iki gazetenin seçilmesi başka bir ifadeyle ister liberal eğilim ister muhafazakar eğilimi temsil etsinler ulusal güvenlik konularında benzer bir söylem izledikleri varsayımına dayanmaktadır.

Araştırmanın tarih aralığı olarak saldırının gerçekleştiği tarih 24 Kasım 2014 başlangıç olarak alınmıştır. Saldırıyla ilgili 24 Kasım-31 Aralık 2014 tarih aralığında yer alan haberler analiz edilmiştir.

Sony Pictures’a yönelik siber saldırıyla ilgili belirlenen tarih aralığında Washington Post İnternet sitesinde 74 haber Washington Times İnternet sitesinde ise 26 haber yer almaktadır.

4. Güvenikleştirme Söylemi ve Siber Uzama Yönelik Güvenlik Söyleminin Temelleri

Son 20 yılda güvenlik çalışmalarında önemli değişimler yaşanmıştır. Siyasi ve entelektüel çevrede yaşanan değişimle birlikte, yeni araştırma gündemleri ve geleneksel olmayan teorik yaklaşımlar güvenlik disiplininin etkilemiştir. Kopenhag Okulu’nun gündeme getirdiği güvenikleştirme fikri bu anlamda önemli bir etki yapmıştır. Bu yaklaşımda geleneksel askeri ve ulusal güvenlik merkezli dar anlamda güvenlik kavramsallaştırılması eleştirilmiş ve güvenliğin neliğine ve nasıl sağlanacağına ilişkin kesin bir tanım oluşturulmasına karşı çıkmıştır. Bunun yerine güvenliğe inşacı bir anlayışla yaklaşılmıştır. Bu anlayışa göre güvenliğe yönelik tehditler keşfedilmesi gereken belirli gerçeklikler olmamalı, güvenikleştirme olarak adlandırılan sosyo-politik bir süreçte söylem aracılığıyla inşa edilmiş olmalıdır.

² <http://libguides.pace.edu/c.php?g=63918&p=410866>

³ https://tr.wikipedia.org/wiki/The_Washington_Post

⁴ http://www.conservapedia.com/Washington_Times

⁵ http://www.sourcewatch.org/index.php/Washington_Times

⁶ http://rationalwiki.org/wiki/The_Washington_Times

Siyasi hayatta, güvenlik söylemleri, politika ve pratiklerin inşası için gündemi şekillendirerek güvenliğe kavramsal bir çerçeve sağlamaktadır. Bu söylemler tehlikelerin inşasında ne objektif ne de analitiktir. Büyük ölçüde tarihi olaylar, güç mücadeleleri ve çıkar farklılıklarına sahip gruplar arasındaki çatışmalardan etkilenirler. Bu nedenle, bu söylemler güvenlik kavramları arasında "alan mücadelesi" olarak adlandırılır (Lipschutz, 1995: 8). Bu mücadelede egemen güçler güvenliği tanımlama hakkını kimin kazanacağını belirlerler, güvenlik söylemlerinin sınırlarını oluştururlar ve sonuçta güvenlikle ilgili sorunlar için kaynak tahsisini kontrol ederler. Güvenikleştirme neoliberal toplumlarda riske tepki vermede tercih edilen yöntemdir. Bir başka ifadeyle neoliberal, ileri kapitalist toplumların, kendi koşullarına uygun hareket ederek, "güvensizlikleri" azaltmak amacıyla risklere yanıt vermenin stratejik bir biçimi olarak anlaşılır (Deisman, 2008: 21). Bir sorun/konu varoluşsal bir tehdit olarak sunulduğunda, konu/sorun güvenikleştirilir. Bu sorunun siyasallaşması, siyasetin normal kurallarının yerini alabilecek derecede aşırı bir seviyeye ulaştığı anlamına gelir. Güvenikleştirme de söz konusu tehditlerle mücadele için acil önlemlerin alınması anlamına gelir.

Güvenikleştirme, güvenliğin, siyasi ve ontolojik olarak verili olduğu, nesnel bir olgu ya da bütün insanların ve devletlerin arzusu olduğu şeklindeki hakim görüşü sorgular. Bu yaklaşımda güvenlik açıkça tanımlanabilen bir nesne ya da belirli bir olgular bütünü olarak değil, sosyal süreçlerin bir ürünü olarak değerlendirilir. Yani, kimin ya da neyin güvenliğinin sağlandığını analiz ederek güvenlik sorunlarının toplumsal olarak inşasına işaret eder. Bir konu/olay mutlaka gerçekten var olan bir tehdit olduğu için değil böyle bir tehditmiş gibi sunulmasından dolayı güvenlik sorunu haline gelir (Neocleous, 2012: 23, 51). Güvenikleştirme, belirli bir kamusal sorunun nasıl ve niçin güvenlik sorununa dönüştüğü konusunun anlaşılması için bize bir alan sağlar. Herhangi bir kamusal sorun siyasal alan dışından siyasal alana oradan da güvenlik alanına uzanan geniş bir yelpazede ele alınabilir. Sorun siyasal alana dahil edilerek kamu politikasının bir parçası haline getirilir. Bu durumda sorun siyasallaşır. Sorunun siyasallaşması da hükümeti bu konuda bir seçim yapmaya ve bu seçimin sonucuna göre karar almaya yönlendirir. Alınan karar sonucunda gerekirse soruna kaynak aktararak sorun toplumsallaştırılır (Miş, 2008: 348).

Siber uzama yönelik güvenikleştirici bir söylemin inşasında uzamın mimari yapısından kaynaklanan risk ve tehditler öne çıkmaktadır. Bu risk ve tehditler siber uzamın teknik özelliklerinden yola çıkarak tanımlanmaktadır. Buna göre siber uzam bilgisayarların biyoelektronik çevresi ve bireylerin teknik altyapısı özellikle de İnternet üzerinden etkileşimde buldukları karmaşık bir sosyo-teknik sistemdir (Kabanov, 2014: 7). Bu karmaşık sosyo-teknik yapı yeni tehditlerin önlenmesinde ezici güç kullanımı ya da güçler dengesini değil, karmaşık ağlarla ilgili iç içe geçmiş politikaları (complex networks of interlocking policies) gerektirmektedir. Siber uzamda meydana gelen güvenlik tehditleri sistem sorunları olarak kavramsallaştırılmakta, bu sorunlarla mücadelede sistem dinamiklerini değiştirmek için yapılan müdahalelerle gerçekleştirilmektedir. Başka bir deyişle, bu yeni savaşlar savaşılmamakta, yönetilmektedir (Bright, 2010).

Siber uzama yönelik güvenlikçi bir söylemin en önemli meşrulaştırıcı araçlarından biri "terörizmle mücadele" söylemidir. Terörizm ve terörizmle mücadele söyleminin merkezinde tehdidin, tehlikenin ve belirsizliğin yorumlanması yer almaktadır. Politikacılar sürekli olarak terör şiddetinin ani, dramatik ve tehdit edici olduğunu, bu nedenle acil eylem gerektirdiğini iddia ederler. Aslında politikacılar tarafından vurgulanan tehlike ve tehdit nesnel bir durum değildir, bu tehlike ve tehditler yetkililer tarafından tanımlanmış, dile getirilmiş ve toplumsal olarak inşa edilmiştir (Campbell, 1998: 1-2). Özellikle tehlike ve tehdit insanlar onları analiz ettiğinde, acil ve yakın olarak düşünüldüğünde gerçekliğe dönüşmektedir. Aslında tehlikeler ve krizler yorumlar aracılığıyla gündeme getirilmekte ve toplumsal olarak inşa edilmektedir (Tsui, 2014: 64-66). Foucaultcu anlamda ele aldığımızda terör tehdidi yorumu terörizm bilgisini oluşturmakta ve terörle mücadeleyle ilgili bir "gerçeklik rejimi" sürdürmektedir. Foucault'ya göre her toplumun kendi gerçeklik rejimi vardır. "Gerçeklik rejimi" kavramı doğru olarak algılanan ve işlev gören bir söylem olarak anlaşılabilir. İktidarlar varlıklarını sürdürebilmek için varlıklarını meşrulaştıracak gerçeklik rejimine ihtiyaç duyarlar. Bu rejimleri oluşturmak için iktidar alanları bilgiyi hem üretir hem de iktidarı besler (Foucault, 2003). Tehlike, tehdit ve savaşın siyasi yorumu bir dizi siyasi amaca özellikle kitlelere yerli ya da yabancı politikaları empoze etmeye hizmet etmektedir. Kamuoyunu olağanüstü çaba ve potansiyel kurbanı hazırlamak için politik ve toplumsal bir tehlike ve tehdit "gerçekliğine" ihtiyaç vardır. Tehdit ve tehlike kavramı da korku duygusu üzerine temellendirilmektedir. Fairclough (1995), Foucault'nun "gerçeklik rejimi" olarak adlandırdığı iktidarların eylemlerini meşrulaştırma stratejisini açıklamada Gramsci'nin "ortak duyu" kavramına başvurur. Fairclough iktidarların söylemlerini meşrulaştırma ve hegemonyalarını sürdürmede "ortak duyu" oluşturarak başarılı olduklarını belirtir. Ortak duyu oluşturularak ideolojiler doğallaşır, saklanır ve gizlenir (Fairclough, 2003b: 171). Ortak duyu hem toplumsal eylemin aracıdır hem de toplumsal eylemin yeniden ürettiği toplumsal ilişkileri kurar (Purvis&Hunt, 2014: 32). "Terörle mücadele söylemi" şu andaki siyasi söylemlerin pek çok çeşidinden biridir. Bu söylem aslında

önemli ölçüde barışçı, insan hakları temelli, feminist, çevresel ya da küreselleşme karşıtlığı gibi alternatif söylemleri bastırarak hegemonik hale gelme girişimidir (Jackson, 2005: 19).

4.1. Medya ve Terörle Mücadele Söylemi

Medya genellikle çağdaş Batı toplumunun önemli bir unsuru olan sosyal bir kurum olarak adlandırılmaktadır. Medya aracılığıyla, toplumsal süreç yorumsal çerçeveler içinde anlatılar ya da hikâyeler yaratır. Bu anlatılar ve hikâyeler toplumsal olarak daha geniş anlamda kültürel ve politik varsayımların içine gömülüdür. Timothy Cook (2001) haber medyasının kendisini politik bir kurum olarak tanımlar. Çünkü haber medyası, diğer politik kurumlarla birlikte Amerikan toplumunun otoriter değerlerinin yerleştirilmesinde önemli bir işleve sahiptir. Sadece kamuoyu ve devlet arasında bir arabulucu olarak hareket etmez aynı zamanda hükümet içinde ve hükümetin bölümleri arasında da arabulucu işlevi görür.

ABD'nin terör saldırılarına reaksiyonunun haber medyası ve popüler kültür tasvirleri/betimlemeleri (depictions) pazarlama, popüler kültür, tüketim ve korku içine batmış bir kültürü ve kolektif kimliği yansıtmaktadır. Elitlerin medya yönetimi ve askeri medya kompleksleri tarafından üretilen propaganda gündelik hayata ve ulusal gündeme yansıyan terör senaryoları üretmektedir. Özellikle 11 Eylül saldırılarından sonra ABD medyasında korku ve belirsiz bir geleceğe vurgu yapılarak terörizmle savaş teşvik edilmiştir (Altheide, 2007: 288-292). Başka bir ifadeyle, 11 Eylül 2001'e dayanarak ABD'nin uluslararası terörizmi "keşfetmesinden" bu yana korkuyu teşvik etmede (promoting) medyanın rolü daha belirgin hale gelmiştir. Korku söylemi, korku politikasına eşlik ederek karar vericileri, vatandaşları korumak adına, vatandaşların "yararına olacak faaliyetleri" kontrol etmede etkin hale getirmiştir. Bu uygulamada risk ve güvenlikle ilgili medya görüntüleri ve temaları merkezi konumdadır. Korku siyaseti, korkuyu artıracak haberleri ve diğer popüler kültür mesajlarını taşıyacak itaatkâr bir medyaya dayanmaktadır. Popüler kültür izleyiciler için devletin bizi korumasını gerektirecek korku, toplumsal kontrol ve senaryolar hakkında anlamlar sağlamaktadır. Korku siyasetinin büyük bir kısmı korku, suç ve terörizm hakkındaki benzer ve tekrarlanan görüntüleri, sloganları teşvik eden kitle iletişim araçlarını kapsamaktadır (Altheide, 2007: 47, 302). Sosyal psikoloji araştırmalarının büyük bölümüne göre belirsizlik ve bilinmeyen genellikle korku ve endişe üretir. Siber terörizm kelimesi de iki önemli modern korkuyu birleştirmektedir: teknoloji korkusu ve terörizm korkusu. Önemli belirsizlikler ve bilinmeyenler, hem teknoloji hem de terörizm bilinen tehditlere göre daha kaygı verici olarak algılanır (Embar-Seddon, 2002: 1034). Debrix'e göre popüler korkuların yeni bir ağırlık ve aciliyet kazanması özellikle 9/11 sonrası Amerika'sında medyayla doyurulmuş toplumlarda gündelik bir rutin haline gelmiştir. Belirsizlik, ortak kaygı ve az ya da çok planlanmış acil durum stratejileri siber terör gibi epifenomenlerin ortaya çıkmasına neden olmuştur. Gerçek ya da hayali tehlikeler olsun bu tür tehdit algıları paranoyit tepkilere neden olmaktadır. Enformasyonun bilgi haline geldiği bir bağlamda, siber terörizmi temsillerinden ayırmanın yolu yoktur (2001: 153). Bu nedenle Amerikan medyası siber terörizmin gerçekliği konusunda konuşmakta oldukça başarılı olmuştur.

Siber uzamın medyada temsili hem korku yaratan hem de tehditleri bildiren anlatılar olarak anlaşılabilir. Medya hikayeleri devamlı geniş kapsamlı ve çeşitli iddiaların üretilmesi için dizayn edilirken, anlatının kendisinin inşası farklı filtreleme süreçlerinin ve editöryel tercihlerin sonucudur. Bu süreçte hikayeye haber değeri kazandırılır (Ericson et al. 1987). Bazı yorumcular ve analistlere göre de medya ticareti "korku söylemi"ne dayanmaktadır. Medya ticareti tehlike ve riskin gündelik hayatın merkezi özellikleri olan hem sembolik hem de edebi (literal) düzeyde iletişim için ayrılmıştır. Medya, resmi sözcülerin konuşmalarına özellikle suç ve tehlikenin inşasında toplumsal denetimin resmi faillerine aşırı bağımlıdır ve risk algısını temsil eden ve güçlendiren medya anlatıları aracılığıyla siber uzamla ilgili tehlikeler inşa edilmektedir. Bu anlatılar hedefledikleri temsilleri kanıtlamak için uzmanların otoritesine başvurmaktadır (Deisman, 2008: 75). Haber medyasının siber terörizm gibi toplumsal bir problemi muğlak ve aşırı geniş bir anlamda kullanması da kamunun bilinmeyene karşı korkusunu besleyerek konunun problematize edilmesine (Entman, 2007), böylece güvenlikleştirilmesine katkıda bulunmaktadır.

5. Söylemsel Ortaklıklar

Metinleri oluşturan söylemler, türler ve tarzlar incelenmeden, söylemsel oluşumların nasıl yeniden üretildiği metinler üzerinden ele alınmadan metinlerin makro düzeyle bağlantısı da kurulamaz. Metinleri oluşturan söylemler, türler ve tarzların incelenmesi bizi metinlerin mezo düzeyde gerçekleştirilen analizine götürür. Mezo düzey analiz bize haber metinlerdeki söylemlerarasılığı analiz etme olanağı sağlar. Söylemlerarasılığın analizi de metinlerdeki ana temaların, temsil edildikleri bakış açılarının belirlenmesiyle gerçekleşir. Böylece hangi söylemsel oluşumların yeniden üretildiği, hangi türlerin, söylemlerin ve tarzların kullanıldığı ortaya çıkarılır. Bu kapsamda incelenen haber metinlerde bir ana tema ve iki yan temanın yer aldığı tespit edilmiştir. Haberlerdeki ana tema ulusal güvenlidir. Yan temalar ise ifade özgürlüğü ve bilgi güvenliği olarak sıralanmaktadır.

5.1. Ulusal Güvenlik Teması

Siber uzama yönelik politikalar ulusal güvenlik endişeleri ve güç çatışmaları ile şekillenmektedir. Doğu Avrupa'da komünist rejimlerin çöküşü ile birlikte Soğuk Savaş sona ermiş, tek süper güç olarak ABD kalmıştır. ABD'nin tek süper güç olarak statüsünü sürdürme yönündeki çalışmaları da hız kazanmıştır. ABD'nin tek süper güç olarak varlığını sürdürebilmesi Mattelart'a göre teknoloji, iktisadi, askeri ve kültürel alanda üstünlüğe dayanmaktaydı. Buna göre ABD'nin yeni küresel hegemonya doktrini hem barış hem de savaş zamanında enformasyon ve iletişim ağları üzerinde kontrolün sağlanmasını gerektirmekteydi. Bu hegemonik doktrininin devamını sağlayan en önemli unsurlardan birisi de nokta operasyona olanak sağlayan "temiz savaş" ya da "sıfır ölümlü savaş" olarak adlandırılan siber savaş söylemidir (2012: 207).

Lawson ve Gehl'e göre Soğuk Savaş sonrası potansiyel tehdit ve güvenlik açıklarının sürekli artan sayısı karşısında, iç ve dış güvenlik arasındaki sınır bulanıklaşmış, ordunun fonksiyonları, kolluk işlevleri, istihbarat örgütlerinin örtüşmesiyle neredeyse günlük yaşamın her yönü güvenikleştirmeye tabi hale gelmiştir. Güvenliğe yönelik potansiyel tehditler çoğalmış, bu yüzden de potansiyel çatışma alanları artmıştır. Siber uzam da bu alanlardan biri olarak yerini almıştır. Siber uzam sadece devlet aktörleri için değil ayrıca devlet adına çalışan devlet dışı aktörler için ya da kendi hesaplarına çalışanlar için de bir araç, bir bölge ya da çatışmanın hedefi haline gelmiştir. Böylece güvenliğin geleneksel üreticileri ve tüketicileri arasındaki sınır bulanıklaşmıştır.

Siber uzama yönelik ve siber uzam kaynaklı tehditler özellikle politika yapıcılar tarafından terörle özdeşleştirilmektedir. Böylece en büyük terör tehdidinin siber uzamdan geleceği ileri sürülmektedir. Bu tehdit kavramsallaştırmasına medya aracılığıyla meşruiyet sağlanmaktadır.

Sony Pictures'a yönelik siber saldırıda terör saldırısı olarak ele alınarak konu ulusal güvenlik bağlamına taşınmıştır. Konunun terör saldırısı olarak çerçeveselenmesinde haber medyası önemli bir işleve sahiptir. Hem Washington Post hem de Washington Times gazetelerinde konuyla ilgili haberlerde saldırıyla ilgili tartışmaların ortak noktası saldırının aslında "ulusal güvenliğe" yönelik bir tehdit olduğudur. Halihazırda saldırıyla ilgili siber güvenlik uzmanlarının, ABD istihbarat birimlerinin, politikacıların saldırıyı terörle ilişkilendirdikleri açıklamalarına yer verilerek saldırının ulusal güvenliğe yönelik bir tehdit olduğu algısı yerleştirilmiştir.

Hem Washington Post hem de Washington Times gazetelerinde Sony Pictures'a yönelik saldırıya ilişkin haber başlıkları incelendiğinde "siber savaş, siber ordu, terör, ulusal güvenlik, siber kabus, 11 Eylül, İnternet altyapısı, güvenlik açığı, FBI, siber güvenlik yasası, savaş eylemi, terör tehdidi, veri güvenliği, siber komutanlık" kelimelerinin kullanıldığı görülmektedir. Bu kelimeler aracılığıyla konu siyasi alana ve ulusal güvenlik alanına taşınmakta, "saldırı, savaş, siber komutanlık" gibi kelimeler aracılığıyla da konunun militarize edilmesi de meşrulaştırılmaktadır.

5.2. İfade Özgürlüğü Teması

Sony Pictures'a yönelik saldırı ve saldırıyı gerçekleştiren hackerlar tarafından yayınlanan tehdit mesajından sonra Interview filminin sinemalara gösteriminin iptal edilmesi ifade özgürlüğüne bir darbe olarak değerlendirilmiştir. Filmin iptalini Washington Post gazetesi "Hackerların Tehdidi Interview Filminin Noel Gösteriminin Rafa Kaldırılmasına Neden Oldu" (Hackers' threats prompt Sony Pictures to shelve Christmas release of 'The Interview'), Washington Times ise "Sony, Kuzey Kore Tarafından Hacklenmesinden ve Terör Tehdidinden Sonra "Interview"i İptal Etti" (Sony kills 'The Interview' after North Korea hack, terror threat) başlığıyla duyurmuştur. Her iki gazete de Obama yönetimi hackerlara karşı gerekli tedbirleri almamakla suçlanmıştır. Saldırı sonrası filmin iptalinin ve hackerlar tarafından filmin gösterilmesi durumunda yeni bir 11 Eylül yaşanacağı uyarısının yarattığı korku ortamının daha sonraki siber saldırılar için cesaret verici olduğu ileri sürülmüştür. Müteakip günlerde de filmin iptalinin eleştirildiği haberler medyada yer almaya devam etmiştir. ABD Başkanı Obama da yaptığı bir basın toplantısında filmin iptalinden dolayı Sony Pictures'ı eleştirmiştir.

Washington Times Obama'nın basın toplantısını duyururken "Obama Sony'i Ortada Bırakmak ve Terör Tehdidini Yönetmekte Başarısız Olmakla Suçlandı" (Obama charged with throwing Sony under bus, failing to lead on terrorist threat) başlığını, Washington Post ise "İnterview'in İptalinden Sonra: Obama Sinemalara Gitmemizi İstiyor" ('Interview' cancellation aftermath: Obama wants us to go to the movies) başlığını kullanmıştır. Washington Times gazetesindeki haberde Sony Pictures'a yönelik saldırının bir ulusal güvenlik sorunu olduğu, bu nedenle Beyaz Saray'ın olaya el atması gerektiği ifade edilmiştir. Washinton Post gazetesinde ise Başkan Obama'nın "sinemalara gitme çağrısı"na dikkat çekilerek ABD'nin temel toplumsal değerlerinden olan ifade özgürlüğüne vurgu yapıldığı değerlendirilmektedir. Her iki haber metninde de Obama'nın filmin iptalini eleştiren açıklamasına yer verilmiştir:

"Biz bir diktatörlüğün bir yerde sansür uygulanmasını empoze edeceği bir toplum olamayız." (We cannot have a society in which some dictatorship someplace can start imposing censorship.) (Washington Times, Washington Post,19 Aralık).

Ancak Washington Post gazetesinde habere Başkan Obama'nın basın toplantısı ve Sony Pictures'la ilgili açıklamasıyla başlanırken, Washington Times gazetesinde habere Obama'nın Sony Pictures'a yönelik saldırı sonrası oluşan kriz durumunu yönetemediğine ilişkin bir siber güvenlik uzmanının görüşüyle başlanmıştır. Bu durum Washington Times gazetesinin daha muhafazakar ve militarist çizgisinin de tezahürü olarak değerlendirilebilir. Her iki gazetede de Interview filminin iptaline yönelik hackleme olayının aynı zamanda mağduru da olan Hollywood aktörleri ve aktrislerinin eleştirilerine yer verilmiştir.

5.3. Bilgi Güvenliği Teması

Sony Pictures'a yönelik saldırı sırasında kendilerini "Barışın Koruyucuları" (Guardians of Peace" (#GOP)) olarak adlandıran hacker grubu tarafından 6 bin 500'ün üzerinde Sony çalışanının e-postaları ile birlikte şifreleri, kredi kartı bilgileri ya da sosyal güvenlik numaraları gibi gizli bilgilerin yer aldığı 100 TB büyüklüğünde veri çalınmıştır. Sızdırılan bilgilerin Hollywood'un en ünlü isimlerine kadar uzanması da saldırının medyatikleşmesini kolaylaştırmıştır. Bilgilerin Amerikan medyasına dağıtılmasından sonra gazetelerin illegal yollardan sızdırılan bu dokümanları haberlerinde kullanmasının etik olup olmadığı yönündeki tartışmalar da başlamıştır. Sony Pictures saldırısı sonucunda paylaşılan gizli bilgiler bilgi güvenliği konusunu yeniden gündeme getirmiştir. Ancak bilgi güvenliği konusunda alınacak önlemlere ilişkin haber metinlerinde siber güvenlik uzmanları, istihbaratçılar, politikacıların görüşlerine yer verilmiştir. Mahremiyet ve gizliliği savunan uzmanlar ya da sivil toplum kuruluşlarının görüşlerine yer verilmemiştir. Böylece bilgi güvenliğinin sağlanması ağ güvenliği ile bağlantılandırılarak kamu-özel işbirliği teşvik edilmiştir. Kamu-özel sektör arasında bilgi paylaşımının artırılmasına olanak sağlayacak yasal düzenleme tekrar gündeme gelmiştir.

Washington Post gazetesinde Sony Pictures'tan sızdırılan, şöhretli kişilere ait spekülasyon bilgileri, politikacılara, şirket çalışanlarına ilişkin bilgilere ve bu bilgilerin medya tarafından haberleştirilmesinin etik olup olmayacağı yönündeki tartışmalara geniş bir şekilde yer verilmiştir. Örneğin bu tartışmalara ilişkin haber başlıklarından birkaçı şöyledir: "Sony İhlali Hollywood Starları Hakkındaki Bilgileri de İçeriyor" (Sony breach included information on Hollywood stars), Sony Hacklemesi ve Maaşların Gizli Tutulmasının Tehlikesi" (The Sony hack and the perils of keeping salaries so secret), "Sony Yöneticisi Amy Pascal Sızdırılan Utanç Verici E-Postalar İçin Özür Diledi" (Sony executive Amy Pascal apologizes for embarrassing e-mails that have leaked), "Sony Hacklenmesi ve Şeffaflık ile İntikam Arasındaki Çizgi" (The Sony hack and the line between transparency and retribution), "Sony Pictures Haber Kuruluşlarını Çalıntı E-Postaları Yok Etmeleri Konusunda Uyardı" (Sony Pictures warns news organizations to destroy 'stolen' e-mails, documents), "Sony Çalıntı Sony Belgelerini Yayınlayan Haber Kuruluşlarını Dava Edecek mi" (Can Sony sue media outlets who publish the stolen Sony documents?) vb.

Daha muhafazakar bir çizgiye sahip Washington Times gazetesinde ise bu tartışmalara çok az yer verildiği tespit edilmiştir. Washington Times'da Sony Pictures'a yönelik saldırılar daha çok güvenlik, terörizm kapsamında ele alınmış, saldırının faili, saldırı karşısında hükümetin tutumuna ilişkin bilgi ve yorumlara yer verilmiştir.

5.4. Metinlerarasılık Bağlamında Haberlerin Değerlendirilmesi

Üretim ve tüketimde metnin geçirdiği değişiklikleri ortaya çıkaran söylem süreçleri Fairclough'un "metinlerarasılık" olarak adlandırdığı çözümleme yöntemiyle ele alınabilir (Gökalp, 2004: 110). Metinlerarasılık kavramı, bir metin ya da metinler grubunun başka metinlerle olan açık ya da gizli ilişkilerini anlatmaktır (Günay, 2007: 211), Fairclough'a (2003) göre ise metinlerin başka metinlerle yaptığı işbirliğidir. Metinlerarasılık, metinlerin nasıl üretildiği, önceki anlayışın nasıl dönüştürüldüğü, mevcut fikirlerin nasıl yeniden yapılandırıldığı ve oluşturulduğuna dikkat çeker. Fairclough için, dilbilimsel analiz doğası itibarıyla betimleyiciyken, metinlerarası analiz daha çok yorumlayıcıdır. Metinlerarasılık metinlerin ikirciliklerinin ve çelişkilerinin kaynağıdır. Söylemler, birer metinlerarasılık ve söylemlerarasılık ürünleridir, tek başlarına durmazlar (Fairclough, 1992: 104). Metinler farklı toplumsal bağlamlarda farklı şekilde tüketilirler. Ayrıca bazı metinler savaşa ya da nükleer silahların imhasına yol açarken bazı metinler ise insanların işlerini kaybetmeleri ya da iş edinmelerine, insanların tutum, inanç ve uygulamalarının değişmesine yol açar (Fairclough, 1992: 78-84, 1995: 59-60)

Haberlerde metinlerarasılık ise dolaylı anlatımlara (reporting speech) örneğin "diğerlerinin" sözlerine metinde yer vermeye dayanmaktadır. Bu anlatım doğrudan aktarım (direct speech) ve dolaylı aktarım(indirect speech) olarak ikiye ayrılır Metin üreticileri doğrudan aktarıma başvurmayı seçtiklerinde açık bir hedef izlemektedirler. Metinlerarasılık kendi amaçlarına uygun olduğu ve metinleri daha ikna edici hale getirdiği için habercilerin hizmetinde güçlü bir araç olarak işlev görür. Ancak dolaylı aktarıma (indirect speech) başvurmada tırnak işaretleri kalkar, zaman ve gösteren yazarın tarzına uyacak şekilde değişir. Biz hiçbir zaman aktarılan ifadenin aktarılan kişiye ait olup olmadığından emin olamayız. Dolaylı aktarımın en önemli handikapı yazara, metni kendi iradesine göre manipüle etme olanağı sağlamasıdır (Seghezzi, 2007).

İncelenen gazetelerin haber metinlerinde doğrudan aktarımın ağırlıkta olduğu görülmektedir. Başkan Obama'nın, Beyaz Saray sözcüsünün, politikacıların, uzmanların görüşleri turnak içinde, doğrudan aktarılmıştır. Bazı hükümet yetkilileri ve istihbaratçıların görüşlerinin aktarılmasında ise dolaylı aktarım yöntemi kullanılmıştır. Haber metinlerinde dolaylı aktarımın nedeni konuşan kişinin ismini açıklamak istememesi olarak ifade edilmiştir.

Doğrudan aktarıma ilişkin örnekler:

Beyaz Saray basın sözcüsü Perşembe günü "Kuzey Kore'nin gerçekleştirdiğinden şüphelenilen Sony Pictures'a yönelik bilgisayar saldırısı "önemli bir ulusal güvenlik meselesidir." dedi. (The suspected North Korea computer attack on Sony Pictures Entertainment is a "serious national security matter," White House press secretary Josh Earnest said Thursday.) (Washington Post, 18 Aralık 2014).

General Alexander milletvekillerine "Dünyada her krizin, olayın ve eğilimin siber yönü vardır. Siber uzamla ilgili kararlarımız fiziksel ya da konvansiyonel faaliyetlerimizi ve yeteneklerimizi de etkileyecektir." dedi. ("Every world event, crisis and trend now has a cyber-aspect to it, and decisions we make in cyberspace will routinely affect our physical or conventional activities and capabilities as well," Gen. Alexander told lawmakers.) (Washington Times, 22 Aralık 2015).

6. Sony Pictures'a Yönelik Saldırının Haber Medyasında Sunumu

Fairclough'a göre metin analizi, metnin dilsel olarak analiz edilmesi demek olup, metindeki kelimeler, gramer yapısı, anlam, ses, cümle seviyesinde uyum analizi yapmayı gerektirir. Dilsel analiz metnin sözcüksel-dilbilgisel ve anlamsal olmak üzere karşılıklı etkiye sahip iki yönünün analizidir. Ayrıca bir metindeki herhangi bir cümle temsil, ilişki ve kimlikler açısından da analiz edilebilir. Yazı bir metinde bir cümleyi analiz ederken analizci;

- Belirli temsiller ve toplumsal uygulamaların yeniden bağlamsallaştırılmaları (düşünsel işlev)-bu pratikler belirli ideolojiler taşıyabilir.
- Belirli yazar ve okur kimliklerinin inşasına,
- Yazar ve okur arasında belirli bir ilişki inşası (örneğin bu ilişkinin resmi ya da resmi olmaması, yakın ya da mesafeli olması gibi)nın nasıl eklemlendiğine dikkat etmelidir.

Analiz sırasında dikkat edilmesi gereken noktalardan birisi de alternatif kelimeler/ifadeler ve bunların ideolojik anlamı/önemidir. Bu tür konular toplumsal ve politik mücadelelerin parçası olarak deneyim alanlarının nasıl başka bir şekilde ifade edildiğiyle ilgilidir. Kelimelerin anlamları ve anlamların daha geniş alana yayılmış mücadelelerle nasıl bir bağlantı kurulduğu dikkat edilecek hususlardan biridir. Fairclough, kelimeler arasındaki ilişkilerin ve bir kelimenin anlamları arasındaki ilişkilerin belirli yapılanmaların hegemonya biçimleri olduğunu söyler (Fairclough, 1995: 57-58, 1992: 73-78)

Metinlerde toplumsal gerçekliğin inşası bize kelimelerin, fikirlerin, kavramların ve inançların nasıl oluşturulduğu, yeniden üretildiği, meydan okunduğu ve yeniden ifade edildiğini ortaya çıkarmamıza yardımcı olur. Geçişlilik belirli dilbilgisi süreçlerinin metinde tercih edilip edilmediği, tema, metin yapısı ve cümle düzeyi temaları arasında benzerlik/uyuşmayı ifade eder, kelime anlamı anahtar kelimelerin anlamına vurgu yapar, üslup, metinlerden metinlere kelime anlamları arasındaki farklılıklara vurgu yapar ve diğer metinlerin aksine metafor metinde kullanılan metaforların özellikleriyle ilgilidir.

Medya metinleri dil aracılığıyla dünyanın temsilini oluştururlar, katkıda bulunurlar ve metinleri oluşturan ve tüketen insanların ideolojileri ve görüşlerinden kendileri de etkilenirler. Dilin bu toplumsal yönü terörizm ve ciddi suçlar gibi olaylarla ilgili tartışmalı metinlerde belirgindir (Markkula, 2014: 7). Haberler siber terörizm "gerçekliği"yle ilişkilerinde karşılıktan ziyade belirleyici/kurucu bir ilişkiye sahiptir. Medya aktif bir şekilde potansiyel güvenlik tehdidinin üretiminde yer alır. David Cambell'e (1998) göre güvenlik nesnel bir durum değildir. Dil, görüntü ve diğer söylemsel uygulamalar aracılığıyla yapılan çerçeveleme ve yorum sonucudur.

Bu bölümde metnin dilsel özelliklerinin tanımlanmasına odaklanılmaktadır. Metinle ilgili olarak kelime bilgisi, başlıklar ve metin yapısına bakılmaktadır.

Siber güvenlikle ilgili haberler gazetelerin daha çok teknoloji ve güvenlik bölümlerinde yer almaktadır. Benzer şekilde Sony Pictures'a yönelik saldırı haberleri de analiz edilen gazetelerde güvenlik ve teknoloji başlıkları altında ele alınmıştır. Sony Pictures'a yönelik saldırının gazetelerin güvenlik bölümlerinde yer alması olayı doğrudan güvenlik çerçevesine yerleştirmektedir. Böylece okuyucunun olaya bakış açısının hangi sınırlar içinde olacağı belirlenmektedir. Yani okuyucunun olayla ilgili haberlerde ulusal güvenlikle bağlantısını kurması, haberlere teknoloji-güvenlik çerçevesinden yaklaşması sağlanmaktadır. Güvenlik çerçevesiyle aslında ABD'nin mevcut güvenlikçi anlayışına uygun olarak kamuoyunda siber uzama yönelik saldırıların tehlikelerine dair bir ortak duyu yaratılmakta, böylece yapılacak yasal düzenlemelere rıza sağlamanın ilk adımı atılmaktadır.

Sony Pictures'a yönelik saldırının failinin Kuzey Kore olduğuna dair kesin kanıtlar olmamasına rağmen fail incelenen gazeteler tarafında Kuzey Kore olarak çerçevelenmektedir. Failin Kuzey Kore

olduđuna dair söylemin inşasında uzmanların, siyasetçilerin ve istihbarat birimlerinin görüşlerinden alıntılara yer verilmiştir. Ayrıca Kuzey Kore liderinin Interview adlı filme yönelik eleştirileri, filmin yayınlanması durumunda yapılacak saldırı tehditleri, 2011 yılında Kuzey Kore tarafından Sony Pictures'a yönelik saldırı failin Kuzey Kore olduđuna dair bir söylemin yerleştirilmesinde temel dayanak noktaları olmuştur. Faille ilgili araştırmada istihbarat kurumları, konuyla ilgili uzmanlar ve hükümet yetkilileri başlıca yetkililer olarak sunulmaktadır. Özellikle konunun güvenlik alanına taşınmasında hükümet yetkilileri ve politikacıların söylemleri haberlerde önemli bir yer işgal etmektedir.

6.1. Başlıklar

Başlıklar haberin en önemli bölümüdür. Çünkü okuyucunun ilgisini artırır ve etkili bir şekilde makalenin içeriğini özetlemeyi amaçlar (van Dijk 1988: 143-144). Gazete haberciliğinin önemli bir ögesi de haber başlıklarıdır. Başlıklar, metni önceden belirlenmiş bir yolda işleyerek okuyucuyu yönlendirmek için oldukça kısa bir şekilde olayın özünü ifade eder. Başka bir ifadeyle başlık okuyucunun metni algılayış şeklini kontrol eder (Teo, 2000: 13).

Tablo 1: Washington Post

Tarih (2014)	Haber Başlığı Türkçe	Haber Başlığı İngilizce
01 Aralık	Kuzey Kore'nin James Franco ve Seth Rogen'a <u>Siber Savaşı</u>	North Korea's cyberwar on James Franco and Seth Rogen
04 Aralık	Araştırmacılara Göre Sony Pictures'a Yönelik Saldırı Kuzey Kore'yle Bağlantılı Görünüyor	Sony Pictures hack appears to be linked to North Korea, investigators say
05 Aralık	Sony İhlali Hollywood Yıldızlarıyla İlgili Bilgileri de İçeriyor	Sony breach included information on Hollywood stars
06 Aralık	Sony Saldırısının Maliyetini Hesaplamak Neden Zor	Why it's so hard to calculate the cost of the Sony Pictures hack
08 Aralık	Kuzey Kore Gibi Ülkeler İçin <u>Siber Ordular</u> Neden İyi Bir Yatırım	Why cyber armies are a good investment for countries like North Korea
11 Aralık	Hollywood'un Hacklenmesi Yeni Bir <u>Siber Güvenlik</u> Tehdidini Vurguluyor	Hollywood gets hacked, highlighting a new cybersecurity threat
14 Aralık	Kuzey Kore ve Sony Hacklemesiyle İlgili Beş Soru (Ve Cevapları)	Five questions (and answers) about North Korea and the Sony hack
15 Aralık	Richard Cohen: Sony E-Mail Skandalı, <u>Siber Kabuslarımız</u> Gerçekleşiyor	Richard Cohen: In the Sony e-mail scandal, our cyber nightmares are coming true
16 Aralık	Sony Pictures Haber Kuruluşlarını "Çalıntı" E-Mail, Belgeleri Yok Etmeleri Konusunda Uyardı	Sony Pictures warns news organizations to destroy 'stolen' e-mails, documents
16 Aralık	"Interview adlı Filmi Gösterecek Sinemaları Tehdit Ederken Sony Pictures Hackerları <u>11 Eylül'ü Hatırlattı</u>	Sony Pictures hackers invoke 9/11 while threatening theaters that show 'The Interview'
17 Aralık	Sony Hack Olayı <u>Güvenlik Açıklarını</u> Ortaya Çıkarırken Gözler Bir Sonraki Kongreye Çevrildi	Eyes turn to the next Congress as Sony hack exposes cybersecurity flaws
18 Aralık	Beyaz Saray Sony Hack Olayının Ciddi Bir <u>Ulusal Güvenlik</u> Sorunu Olduđunu Söyledi	White House says Sony hack is a serious national security matter
19 Aralık	Hackerlar <u>İnternet Altyapısının</u> Peşinde	Hackers are going after the Internet's very infrastructure
19 Aralık	Kuzey Kore Sınırlı Bir İnternete Sahip. Ve Bu Durum <u>Siber Savaşta İyi Bir Savunma Yöntemi Olabilir</u>	North Korea barely has the Internet. And that could be good defense in a cyberwar,
19 Aralık	Kuzey Kore'nin <u>Terör</u> Mirası Hacklemenin Ötesinde	North Korea's legacy of terrorism goes far beyond hacking
23 Aralık	Açıklama: Sony ve Interview'e Siber Saldırıdan <u>Ulusal Güvenlik</u> Konusunda Alınacak Dersler	Commentary: Lessons in national security from the cyber attack on Sony and 'The Interview'

Tablo 2: Washington Times

Tarih 2014)	Haber Başlığı Türkçe	Haber Başlığı İngilizce
2 Aralık	Druge Raporuna Göre, FBI'nın Sony Uyarıları Sırasında WND Hizmet Dışı Kaldı	Drudge Report, WND go dark amid FBI warning of Sony hack
4 Aralık	Uzmanlar Sony Saldırısıyla Güney Kore'ye Yönelik Saldırı Arasında Paralellik Gördüler	Experts see Korean parallels in Sony hack
16 Aralık	<u>Siber Güvenlik Yasası</u> Zayıf Kaldığından Sony Hackerları Terör Tehdidini Artırdı	Sony hackers up ante with terrorist threat as cybersecurity bill languishes
17 Aralık	Sony, Kuzey Kore Tarafından Hacklenmesinden ve Terör Tehdidinden Sonra "Interview"i İptal Etti	Sony kills 'The Interview' after North Korea hack, terror threat
18 Aralık	Artçı Saldırılarıyla Bir <u>Siber Savaş</u> , Tali Hasar ve Öfkeli Büyük Bir İzleyici	A cyberwar with aftershocks, collateral damage and a big angry audience
18 Aralık	Newt Gingrich Kuzey Kore'nin Sony'i Hacklemesini <u>Bir Savaş Eylemi</u> Olarak Adlandırdı	"Newt Gingrich calls North Korea's Sony hack 'an act of war'
18 Aralık	John McCain Sony Saldırısında Obama'yı İlgisiz Davranmakla Suçladı	John McCain blames Obama for lax cybersecurity in Sony hack attack
19 Aralık	Sony Hacklenmesinde FBI Resmi Olarak Kuzey Kore'yi Suçladı	FBI formally blames North Korea in Sony hack
19 Aralık	Sony Saldırısından Sonra Şirketlerin Veri Güvenliği	Companies' data security in question after

	Sorgulanıyor	Sony hack
22 Aralık	Siber Komutanlığa Yatırım ABD'den İntikam Almayı Hedefleyen Hackerlar Karşısında Teminattır	Cyber Command investment ensures hackers targeting U.S. face retribution.
25 Aralık	Sony Saldırısının Ortasında Rağmen Rusya Kuzey Kore'ye Destek Vermeyi Teklif Etti	Russia offers support to North Korea amid Sony hack

Her iki gazete de yer alan haber başlıkları siber uzama yönelik yeni bir güvenlik yasasının gerekliliğine vurgu yapmaktadır. ABD'de uzun süredir özel sektörle bilgi paylaşımının geliştirilmesine ilişkin bir yasanın gerekliliğine ilişkin tartışmalar sürmektedir. Amerikan hükümeti tarafından 2009 yılında yayınlanan Siber Güvenlik Politika Değerlendirmesinde de özel sektörle bilgi paylaşımının gerekliliğine vurgu yapılmıştır. Ancak özel sektörün hassas bilgiyi hükümetle paylaşmasının önündeki en büyük engel bilgi paylaşımının "itibarın zarar görmesi, sorumluluk ya da düzenleyici sonuçları" olabileceği korkusudur (2009: 19). Başka bir ifadeyle, bilgi paylaşım rejimlerinin varlığı ihtiyaç durumunda özel sektör için temel bir husus olan bu alanlarda hükümetlere daha fazla düzenleme fırsatı verebilir. Özel sektör için diğer bir endişe kaynağı da, olayı rapor etmenin pay sahiplerinin eylemlerinde nedensel etkileriyle pazar reaksiyonlarını riske edebileceğidir (Cyber Security Review, 2009). Konu zıt yönde de çalışabilir, yani hükümetin hassas istihbarat bilgileri özel sektörle paylaşması "bireylerin ve toplumun" gizlilik hakkını ihlal edebilir (2009: 19). Bütün bu çekincelere rağmen Sony Pictures'a yönelik saldırı devlet-özel sektör bilgi paylaşımını düzenleyen yeni bir siber güvenlik yasasının gerekliliğini gündeme getirmiştir. ABD'nin siber güvenlik belgelerindeki "siber uzama yönelik uluslararası bir düzenlemenin gerektiği" yönündeki çağrısı hukukçular tarafından tekrar gündeme getirilmiştir (Kesan, 2015).

Saldırıdan bir ay sonra Başkan Obama Kongre'ye hükümet ile özel sektör arasında daha büyük bilgi paylaşımının yolunu açan yeni bir siber güvenlik kanun tasarısı getireceğini ilan etmiştir. Yasanın "kişilerin özel hayatı ve özgürlüğünü koruma altına alınması" gibi unsurları içereceği açıklanarak⁷ yasaya yönelik ulusal kamudan gelecek eleştirilerin önlenmesi amaçlanmaktadır.

Sony Pictures'a yönelik haberler ABD hükümeti tarafından uzun süredir gerçekleştirmek istenen ama başarılı olunamayan hem devlet-özel sektör arasındaki bilgi paylaşımı hem de uzama yönelik uluslararası yasal düzenlemenin gerekliliği konusundaki mevcut söylemin meşruiyet kazanması yönünde önemli bir adım olmuştur.

Güvenikleştirme söyleminde "savaş, ulusal güvenlik, saldırı, terör" gibi kelimeler güvenikleştirme meşrulaştırma araçlarıdır. Hem Washington Post hem de Washington Times gazetelerinde konuyla ilgili haber başlıkları aracılığıyla Sony Pictures'a yönelik saldırı ulusal güvenlik sorunu olarak çerçevelenmiştir. Terörle mücadele söyleminin ana teması olan ulusal güvenlik söylemine göre enformasyon teknolojilerine bağımlılık nedeniyle bir bütün olarak toplumun temel değerleri tehlike altındadır. Tehdide karşı uygulanan hareket biçimlerinin teknik düzey, yasal mevzuat, kurumsal ya da uluslararası olmak üzere çeşitli düzeyleri vardır. Temel aktörler güvenlik uzmanlarıdır. Temel tehdit teröristlerdir.⁸ Aslında "terörle mücadele söylemi" şu andaki siyasi söylemlerin pek çok çeşidinden biridir. Önemli ölçüde barışçı, insan hakları temelli, feminist, çevresel ya da küreselleşme karşıtlığı gibi alternatif söylemleri bastırarak hegemonik hale gelme girişimi (Jackson, 2005: 19) olarak değerlendirilebilir.

⁷"Obama siber güvenlik paketi açıkladı", Sabah gazetesi, 14 Ocak 2015, <http://www.haberturk.com/dunya/haber/1030206-obama-siber-guvenlik-paketi-acikladi>.

⁸ A Comparative Analysis of Cybersecurity Initiative Worldwide. WSIS Thematic Meeting on Cybersecurity. Geneva, 28 June-1 July 2005. http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf

Haberlerde Sony Pictures'a yönelik saldırının çerçevelenmesinde "savaş" metaforunun kullanım sıklığı dikkat çekicidir. Metafor kavramı politik söylemin dinamiklerine ilişkin içgörü sağlar. Geleneksel olarak, metaforlar kelimeler, dilde dekoratif, eğlenceli ve ikna edici fonksiyonları için kullanılan fikirler, cümleler olarak kabul edilir. Son zamanlarda, özellikle Foucault'nun söylem teorisinde, bir metafor, söylemin üretiminin kontrol edildiği, seçildiği, organize edildiği ve yönlendirildiği bir sosyal pratik olarak görülür (Maasen&Weingart, 2000: 21). Bu nedenle metaforlar güç/bilgi etkileşimde etkin unsurlar haline gelmişlerdir. Hackerların 11 Eylül 2001 tehdidi ABD toplumunun yaşadığı felakete atıfta bulunarak, ABD'nin "Dijital 11 Eylül" korkusunu pekiştirmektedir. Böylece geleneksel güvenlik önlemlerinin siber uzama uygulanmasının da önü açılmıştır. Fairclough'a göre modern medya söylemi yoğun bir şekilde 11 Eylül 2001 saldırıları ve sonrasında etkilenmiştir. Fairclough'a (2003) göre 11 Eylül sonrası terörizm dış güçlerle bağlantılandırılmıştır. "Savaş" metaforunun kullanılması aslında ABD'de sürdürülen terörle mücadele söyleminde yaygın bir gelenektir. Bu gelenek 1980'li yıllarda Reagan döneminde başlamıştır. Chin-Kuei Tsui, 2014 yılında tamamladığı "Tracing the Discursive Origins of the War on Terror: President Clinton and the Construction of New Terrorism in the Post-Cold War Era" başlıklı doktora çalışmasında Soğuk Savaş sonrası dönemdeki ABD'nin terörle mücadele söylemini ve savaş metaforunun kullanımını, söylemin Başkanlara göre değişiklik gösterip göstermediğini incelemiştir. Tsui ağırlıklı olarak Bill Clinton ve George W. Bush dönemi terörle mücadelede savaş metaforu kullanılarak oluşturulan söylemi incelediği çalışmasında aslında bugün ABD'de halen sürdürülen yaklaşımı 1980'lere Ronald Reagan dönemine kadar götürebileceğimizi ileri sürmektedir. Öyle ki Obama döneminde resmi belgelerde "terörle savaş" söylemine başvurulmayacağı açıklansa da ufak değişikliklerle Obama'nın da Bush dönemi söylemini devam ettirdiği görülmektedir.

Kısaca medya aracılığıyla inşa edilen terör tehdidi ve terörle mücadele söylemi terörizm hakkında bir "ortak duyu" inşa etmeye hizmet etmekte, ABD'nin terörle savaş söyleminin politik gerçekliğini oluşturmakta ve mevcut yönetimin terörle mücadele söylemini meşrulaştırmaktadır. Terörle savaş söyleminin "terörle sürekli savaş" söylemine dönüştüğü 11 Eylül saldırıları, 11 Eylül sonrası ABD'nin ulusal güvenliğinin sağlanması açısından hem içte hem de dışta yoğun şekilde silahlanmayı ve önleyici tedbirlerin yolunu açmıştır (Harvey, 2007). Siber uzama yönelik bir terörle mücadele ya da savaş söyleminin ulusal güvenlik kapsamında uzama yönelik askeri yatırımların artmasına neden olacağı değerlendirilmektedir.

6.2. Kelime Bilgisi

Kelime bilgisi bir metnin tamamını, tek tek kelimeleri ve bunların anlamını kapsar (Fairclough, 2003). Sony Pictures'a yönelik saldırıyı tanımlamada siber savaş, ulusal güvenlik, siber terörizm, siber silahlar, kritik altyapı kavramları güvenikleştirme söylemine ilişkin temel çerçeveyi çizmektedir.

Bazı kelimelerin, özellikle negatif çağrışıma sahip olan kelimelerin tekrar edildiği görülmektedir. Bu kelimeler okuyucuda korku yaratma stratejisinin bir parçasıdır. Haberlerde özellikle negatif çağrışıma sahip "terörizm, savaş, caydırıcılık, saldırı, intikam, suç konusu, düşman güçler, siber ordu, risk altında olmak" gibi kelimeler sıklıkla kullanılmaktadır.

Siber uzama yönelik tehditlerin risk çerçevesinden meşrulaştırıldığı risk yaklaşımında düşman belirsizdir, tehlikenin nereden geleceği tahmin edilemez. Tehlike tüm ulusa yönelikmiş gibi inşa edilir. Tehlikeli "öteki" kolektif bir benlik olarak ulus düşüncesini üretir. "Bizim bilgisayarlarımız" ya da "bizim altyapımız" gibi ortak ifadeler bu etkiyi artırır. Bu nedenle saldırılara karşı savunma ulusal güvenlik politikasının görevi olarak sunulur. Haberlerde Kuzey Kore olarak tanımlanan failin harekete geçmesinde intikam, korku yaratma ve mesaj verme kaygılarının öne çıktığı resmedilmektedir. Böylece Sony Pictures'a yönelik saldırının aslında "biz" olarak adlandırılan Amerikan toplumu ve bu toplumun yapılarının güvenliğini tehdit ettiği imlenmektedir.

Sonuç

Sony Pictures'a yönelik siber saldırı örnek olayından hareketle siber uzama yönelik saldırıların ABD medyasında sunumunun incelendiği bu çalışmada Washington Post ve Washington Times gazetelerinin İnternet sitelerinde yer alan saldırıyla ilgili haberler analiz edilmiştir.

Haberlerin söylemsel olarak inşasında risk ve tehdit algısından yola çıkılarak bir korku ortamı oluşturulduğu görülmektedir. Sony Pictures'a yönelik siber saldırı haberler aracılığıyla bir terör saldırısı olarak çerçevelenmiş, böylece konu "ulusal güvenlik" kapsamına taşınmıştır. Başka bir ifadeyle Sony Pictures'a yönelik siber saldırının haber medyasında temsili pek çok politika belgesinin başaramadığı şeyi yaparak "ulusal siber güvenliğin" önemini gündeme getirmiştir. Hem Washington Post hem de Washington Times gazetelerinde konuyla ilgili haberlerde saldırıyla ilgili hakim tema "ulusal güvenlik" temasıdır. Saldırı "ulusal güvenliğe" yönelik bir tehdit olarak çerçevelenmiştir. Bu çerçevelenmenin başarıya ulaşmasında hükümet yetkililerinin, istihbarat birimlerinin ve siber güvenlik uzmanlarının görüşleri birincil derecede etkili olmuştur.

Siber savaş, siber ordu, terör, ulusal güvenlik, siber kabus, güvenlik açığı, savaş eylemi, terör tehdidi gibi negatif çağrışımlara sahip kelimelerin kullanımı aracılığıyla konu ulusal güvenlik ve dolayısıyla askeri alana taşınmıştır. Böylece konunun militarize edilmesi süreci hızlandırılmıştır.

Muhafazakar bir eğilime sahip Washington Times ve liberal bir eğilime sahip Wshington Post gazetesinin, Sony Pictures'a yönelik siber saldırıyı egemen ideolojiyle uyumlu bir şekilde siber terörizm kapsamında ele almıştır. Başka bir ifadeyle her iki gazetede de temelde ulusal güvenlikle ilgili bir konuda benzer bir söylem kullanılmış, Sony Pictures saldırısına yönelik söylemsel inşasında güvenlikçi anlayışın hakim olması uzamın güvenlikleştirilmesine meşru bir zemin sağlamıştır.

Siber terör tehdidinin medya aracılığıyla inşasının yarattığı korku ortamı uzama yönelik yeni düzenlemelerin önünü açmıştır. Kamu-özel sektör arasında bilgi paylaşımının artırılmasına olanak sağlayacak yasal düzenleme tekrar gündeme gelmiştir. Böylece mevcut ideolojiyle uyumlu şekilde bilgi paylaşım yasasının gerekliliğine yönelik kamuoyunda bir ortak duyu oluşturulmuştur. Haberlerde alternatif ya da muhalif seslere yer verilmemesi de bu inşa sürecini kolaylaştırmıştır.

Saldırı ifade özgürlüğüne bir darbe olarak nitelendirmekle birlikte kişi hak ve özgürlüklerini, gizlilik ve mahremiyetini ihlal eden düzenleme tekrar gündeme getirilmiştir. Bilgi güvenliği tartışılmakla, birlikte kişi hak ve özgürlüklerinin ihlali kapsamında değerlendirilebileceğimiz "gizlilik ve mahremiyeti" tehlikeye atan bilgi paylaşım yasası meşrulaştırılmaya çalışılmıştır. Bu meşrulaştırma sürecinde ise Amerikan toplumunun tarihsel travmalarına atıf yapan metaforlara başvurulmuştur.

Siber terörizm olarak çerçevelenen Sony Pictures'a yönelik siber saldırı Amerikan yaşam tarzına yönelik bir tehdit olarak sunulmuştur. Amerika ve temsil ettiği değerlerin (ifade özgürlüğü ve demokrasi) yıkımını görmek arzusuyla motive edilmiş bir saldırı olarak karakterize edilmiştir. Böylece teknoloji ve terörizm korkusu bir potada birleştirilmiştir.

KAYNAKÇA

- ALTHEIDE, David (2007). "The Mass Media and Terrorism", *Discourse & Communication*, C. 1, S. 3, s. 287-308, doi: 10.1177/1750481307079207, (15.04.2015).
- BIÇAKÇI, Salih (2013). 21. Yüzyılda Siber Güvenlik, İstanbul: İstanbul Bilgi Üniversitesi Yayınları.
- BRIGHT, Jonathan (2010). "Security, Technology and Control: Repositioning Securitisation Theory for the Information Society", *Politics in Hard Times: International Relations Responses to the Financial Crisis*, SGIR 7th Pan-European Conference, Stockholm, www.eisa-net.org, (15.10.2015).
- CAMPBELL, John (2002). "Ideas, Politics and Public Policy", *Annual Review of Sociology*, S. 28, s. 21-38, DOI: 10.1146/annurev.soc.28.110601.141111, (12.01.2015).
- CAMPBELL, David (1998). *Writing Security: United States Foreign Policy and the Politics of Identity*, Manchester: University Press.
- COOK, Timothy (2001). "The Future of the Institutional Media", *Mediated Politics*, Lance Bennett, Robert M. Entman (ed.), New York: Cambridge University Press.
- DEISMAN, Wade (2008). *Securing Cyberspace: Neo-Liberalism, Risk And Child Safety*, Yayınlanmamış Doktora Tezi, Ottawa: Carleton University.
- ENTMAN, R. Mathew (2007). "Framing Bias: Media In The Distribution Of Power", *Journal of Communication*, C. 57, S. 1, s. 163-173.
- ERİKSSON, Johan, GIACOMELLO, Giampiero (2007). "Closing the Gap Between International Relations Theory and Studies Of Digital-Age Security", *International Relations and Security in the Digital Age*, Johan ERİKSSON, Giampiero GIACOMELLO (ed.), London ve New York: Routledge, s. 1-28.
- FAIRCLOUGH, Norman (1992). *Discourse and Social Change*, UK: Polity Press.
- FAIRCLOUGH, Norman (1995). *Critical Discourse Analysis: The Critical Study Of Language*, London: Longman Group Limited.
- FAIRCLOUGH, Norman (1996). *Language and Power*, New York: Longman.
- FAIRCLOUGH, Norman (2003). *Analysing Discourse: Textual Analysis For Social Research*, London: Longman Group Limited.
- FOUCAULT, Michel (2003). "İktidar ve Beden", *İktidarın Gözü, Seçme Yazılar 4*, İstanbul: Ayrıntı Yay, s. 38-47.
- FOWLER, Roger (1991). *Language In The News: Discourse And Ideology In The Press*, London: Routledge.
- GÖKALP, Emre (2004). *Türkiye'de Spor Basını ve Milliyetçilik Söylemi*, Yayınlanmamış Doktora Tezi, Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü.
- GÜNAY, Doğan (2013). *Söylem Çözümlemesi*, İstanbul: Papatya Yayınevi.
- HARVEY, David (2008). "The Right To The City", *New Left Review*, S. 53, s. 23-40.
- JACKSON, Richard (2005). *Writing the War on Terrorism: Language, Politics and Counterterrorism*, Manchester, UK: Manchester University Press.
- KABANOV, Yury (2012). *Information (Cyber-) Security Discourses and Policies in the European Union and Russia: A Comparative Analysis*, Working Paper, <http://publications.hse.ru/en/preprints/143476248>, (15.01.2015).
- KESAN, Jay (2015). *UI Legal Scholar Discusses The Recent Cyber Theft From Sony Pictures*, <http://illinois.edu/lb/article/391/89807>, (15.10.2015).
- LAWSON, Sean, GEHL, Robert (2011). "Convergence Security: Cyber-Surveillance and the Biopolitical Production of Security" *Cyber-Surveillance in Everyday Life: An International Workshop*, May 12-15, University of Toronto, <http://www.digitallymediatedsurveillance.ca/wp-content/uploads/2011/04/Lawson-Gehl-Convergence-Security.pdf>, (15.01.2014).
- LIPSCHUTZ, Ronnie (1995). *On Security*, New York: Columbia University Press.
- MARKO, Daver (2013). "Fear Control in Media Discourse", *Southeastern Europe*, S. 37, s. 200-219.
- MARKKULA, Sampsa (2014). *Crime, Terrorism or Nightmare: News Representations of the 2011 Norway Attacks*, Yayınlanmamış Yüksek Lisans Tezi, Finland: University of Jyväskylä.
- MATTELART, Armand (2012). *Gözetimin Küreselleşmesi- Güvenleştirme Düzenin Kökeni*, İstanbul: Kalkedon.
- MİŞ, Nebi (2008). "Güvenleştirme Teorisi ve Siyasal Olanın Güvenleştirilmesi", *Akademik İncelemeler Dergisi*, C. 6, S. 2, s. 346-381.
- NEOCLEOUS, Mark (2012). *Güvenlik, Şiddet ve Savaş*, Ankara: Dipnot Yayınları.

PURVIS, Trevor, HUNT, Alan (2014). "Söylem, İdeoloji, Söylem, İdeoloji, Söylem, İdeoloji...", *Moment Dergi*, C. 1, S. 1, s. 9-36, DOI: <http://dx.doi.org/10.17572/mj2014.1.936>, (15.03.2015).

SEGHEZZI, N. Andrea (2007). "Intertextuality in the News: The Spanish Terrorist Attack on March 11", *Revista Alicantina de Estudios Ingleses*, C. 20, s. 195-221 doi=10.1.1.471.8190&rep=rep1&type=pdf, (14.04.2015).

TEO, Peter (2000). "Racism In The News: A Critical Discourse Analysis Of News Reporting In Two Australian Newspapers", *Discourse & Society*, C. 11, S.1, S. 7-49.

TSUI, Chin-Kuei (2014). Tracing the Discursive Origins of the War on Terror: President Clinton and the Construction of New Terrorism in the Post-Cold War Era, Yayınlanmamış Doktora Tezi, New Zeland: University of Otago, <hdl.handle.net/10523/4771>, (14.05.2014).

VAN DİJK, Teun (1998). *Ideology*, London: Sage.

www.washingtonpost.com

www.washingtontimes.com